

# Reengineering a monitor for Usage Control at the Operating System level

## Hiwi assignment

Supervisors: Enrico Lovat, Prof. Dr. Alexander Pretschner

Email: {enrico.lovat, alexander.pretschner}@kit.edu

Phone: +49 721 608 5192

Starting date: immediately

Prerequisites: 'C' programming language; basic knowledge of logics would be an added advantage

### Introduction

Usage control requirements specify restrictions and compulsory actions that relate to the future handling of data. The enforcement of such requirements can and must happen at different levels of abstraction within a system, like windowing system, operating system, service level, etc. This is because the same data have different representations at different levels, as well as the same actions, like "copy" or "delete", have different semantics. In order to control the usage of a specific data, we need to monitor and track actions performed over all of its representations.

This work addresses the problem at the operating system level, by enforcing usage control via system calls interposition. Our current system intercepts (via the SysTrace tool) every system-call triggered inside a sandboxed shell and allows the execution only when the latter doesn't generate a violation of any of the policies loaded at boot-time.

### Work package

The goal of this assignment is to reengineer the current version of the monitor we have, tailored on a specific version of OpenBSD, and make it portable to other Linux system.

Submission of the following is mandatory at the end of the assignment:

- (i) Raw (commented) code
- (ii) Compiled version of the XPCOM object
- (iii) Virtual machine(s) for demo of the work
- (iv) Documentation explaining the set up and usage of the code and the virtual machine(s)

### Work Plan

1. Read and understand the documentation about Usage Control at the Operating System level
2. Familiarize with the existing implementation.
3. Complete the work package.
4. Submit the work as explained above.

### References and further readings

- [1] Harvan, M., Pretschner, A.: State-based Usage Control Enforcement with Data Flow Tracking using System Call Interposition [http://sec.cs.uni-kl.de/index.php/component/docman/doc\\_download/87-nss09](http://sec.cs.uni-kl.de/index.php/component/docman/doc_download/87-nss09)
- [2] Systrace, <http://www.citi.umich.edu/u/provos/systrace/> [Accessed: October 13, 2010]